

Manage users the easy way

Microsoft's Active Directory is the best way to manage all your users and IT equipment, as well as enforcing a security policy. Karl Wright shows you how it's done

If there's no central server on your network, a password has to be created individually for every resource on the network (or those resources must be left unprotected, creating a security risk for your business). This makes managing and updating passwords time consuming and difficult.

In a network managed by an Active Directory domain controller, each user needs only one Active Directory user account, and hence only one username and password, with a user's rights to resources on the network associated with this account. This is a far more logical approach to network administration. It makes user management much easier, allowing you to control access to a greater range of resources without becoming bogged down in keeping track of, and updating, potentially hundreds of resource-level passwords.

If you have a shared folder on a PC that is part of a network with no central server, you can choose to share that folder with everyone, or to limit access to specified users. However, you can grant access only to the user accounts that reside on the PC. If you want John in accounts to be able to access the finance folder on your account manager Tania's PC, Tania's PC will need a user account for John that has exactly the same password as John's user account on his own PC. Not only is this incredibly inefficient and confusing if you have more than a few users, it's also a security risk. Using Active Directory, you can give different users on the network different levels of access to a shared folder using only their centrally stored user accounts.

In this article, we'll show you how to use Active Directory to make your network more secure, easier to manage and work harder for your business.

DESIGNING AN ACTIVE DIRECTORY STRUCTURE

An Active Directory database is broken down into a number of different sub-units, each with its own

particular function. At the top of the organisational structure is the domain to which all the resources administered by your server (referred to as the domain controller) belong.

One level further down are the Organisational Units (OUs). OUs are the smallest sub-unit to which you can directly apply a Group Policy Object (GPO), the main Active Directory configuration tool. Because of this, it can be tempting to create lots of OUs – one for each logical subdivision of your network or your business, for instance. However, unless you are very careful about how you design your Active Directory structure, this can create more problems than it solves. If you try to configure an OU in a way that contradicts existing settings, something that becomes increasingly likely the more OUs you have, then your changes simply won't take effect and you'll be left scratching your head wondering why.

For the purposes of this article, we created an Active Directory design for a company with two partners, two network administrators, two finance people, a warehouse department and several other employees. We didn't create any new OUs. Instead, we used the default MyCompany OU and created security and distribution groups corresponding to the different functions within the company.

Groups are the next sub-unit down from OUs. You can't apply a GPO to a group. Instead you apply the GPO to the OU of which the group is a member. You can then use security filtering to ensure that the GPO's settings apply only to a particular group of users or computers within the OU. Active Directory groups can also be added to Access Control Lists (ACLs), giving very precise control over relatively small groups of users.

Next to GPOs, ACLs are the second most important configuration tool within Active Directory. Each resource has its own ACL, detailing who can use it and in what manner. In order to keep your Active Directory structure as simple and clean as possible, you should try whenever possible not to specify permissions on a user-by-user basis. If you have any more than a handful of users, this will quickly make network administration more complicated than it needs to be.

Here we are going to show you how to create groups and Group Policy Objects, how to link GPOs to OUs and then use security filtering to make sure that the GPO applies only to a specific group within the OU.

CREATING A GROUP IN ACTIVE DIRECTORY

In the Windows Start menu, go to All Programs, Administrative Tools, and open Active Directory Users and Computers. In the Users and Computers snap-in, expand your domain and then under the domain find the OU called MyBusiness. Within MyBusiness click the OU called Security Groups. Right-click in the right-hand pane of the Users and Computers snap-in and select New and then Group from the Windows Context Menu.

INTRODUCTION

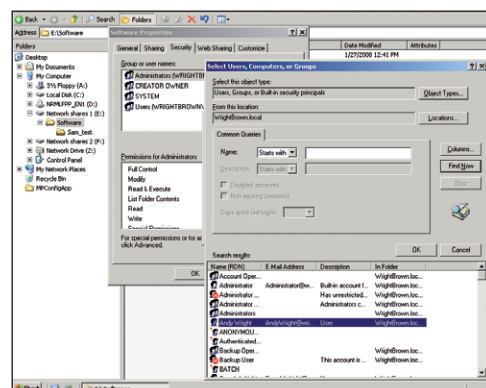
Following on from last month's introduction to installing Windows Small Business Server, this month we'll explain how to configure Active Directory. This is a database that contains all the information about your network and its resources, including servers, PCs, users, printers and shared folders. It contains all your security permissions and information on what users are allowed (and not allowed) to do.

This gives you a single point of management for your entire network, making it easy to control how your entire network infrastructure works. We'll show you how to manage it correctly.

Karl Wright
IT Correspondent



karl@computershopper.co.uk



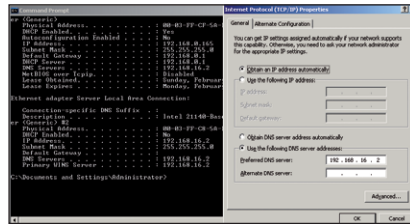
▲ One of the key components of Active Directory, the ACL is a list of permissions detailing who has what rights to use a resource such as a shared folder, a printer or even a Group Policy Object



Domain name games Configuring Active Directory and DNS

In order to match resources such as a named printer or PC to an IP address, most networks use something called a domain name server (DNS). To make sure your server and clients interact as you intend them to, there are a few things you need to know about DNS. First, clients should be configured to use your domain controller as their DNS. Second, and less obviously, your domain controller should be configured to act as its own DNS server.

To map specific services on the network to the domain controller providing that service, Active Directory needs to register SRV



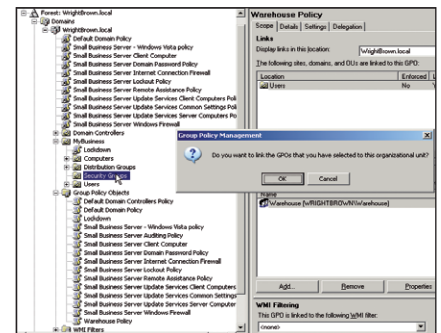
▲ Make sure that your server is set up to use itself as a DNS or your clients may have difficulty resolving some services on your network

records with the domain controller's DNS service. This can't be done if your domain server is configured to use your ISP's DNS.

At this point, you're probably wondering how your server and the clients attached to it will access the internet if they're all using your server; you need to specify your ISP's DNS as a 'forwarder', which is able to resolve queries that your own DNS can't. This can be done in the DNS management snap-in under Administrative Tools on the Windows Start menu.

However, if you run the Internet Setup wizard as soon as Windows Small Business Server has finished installing, then the forwarder will be automatically configured for you.

The tools that are most used to work with Active Directory are the Group Policy Management snap-in and the Active Directory Users and Computers snap-in. In the main article, we show you how to use these applications to apply a GPO to an organisational unit and then restrict the effect of that GPO to a single security group.



▲ Linking a Group Policy Object to an organisational unit is easy. Just open the Group Policy Management snap-in, select the GPO and then drag and drop it on to the OU in question

USING SECURITY FILTERING

In the Group Policy Management snap-in, drag your GPO from its folder and drop it on to the OU that contains the group to which you want the GPO to apply. In our case, we drag and drop the Warehouse Policies GPO on to the Users OU. This links the GPO to the OU.

At this point, the GPO still applies to the whole OU (all the users in our domain), so select the GPO in the Group Policy Management snap-in. In the bottom half of the right-hand pane you'll see something called Security Filtering. This is the Access Control List for the GPO you have just created. Currently, the only entry on this ACL is Authenticated Users (everyone in the OU). Remove the entry for Authenticated Users from the Security Filtering ACL and click on the Add button. Just as you previously added users to your Warehouse Security Group, go through the same steps to add the Warehouse Security Group to the ACL for the Warehouse Policy GPO.

While you're in the Group Policy Management and with your GPO selected, click the Delegation tab. Select your group in the Access Control List and click Advanced in the pane's bottom right-hand corner. Make sure your Security Group has ticks next to the Read and Apply Group Policy permissions. Now click your way out of the Group Policy Editor. You will find that your changes apply only to members of the group specified when configuring security filtering. **ES**

CREATING A GROUP POLICY OBJECT

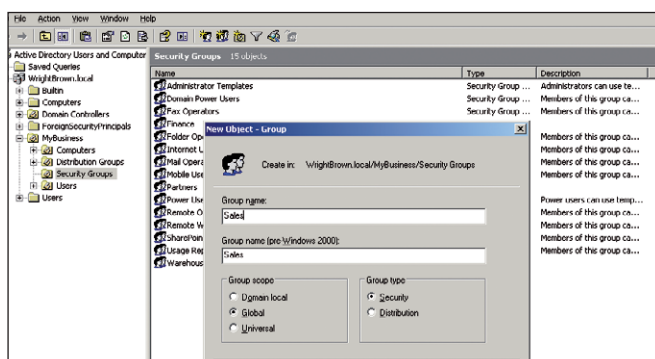
From the Administrative Tools folder in the Windows Start menu, open the Group Policy Management snap-in. In the left-hand pane of the snap-in, right-click the Group Policy Objects container, select New from the context menu and give your GPO a meaningful name. In our example, we called the GPO Warehouse Policy. Your GPO will appear in the GPO list. Right-click it and choose Edit from the Context Menu to open the Group Policy Object Editor.

In the Group Policy Object Editor, under User Configuration, expand Administrative Templates. Select one of the folders you find here and, in the right-hand pane, a list of settings will appear. In our example, we have decided that the warehouse staff shouldn't be able to access the Windows Control Panel, so we've selected the Control Panel folder in the left-hand pane and then in the right-hand pane enabled the setting Prohibit access to the Control Panel. In real-life, however, you'd be unlikely to create a GPO just to apply a single setting.

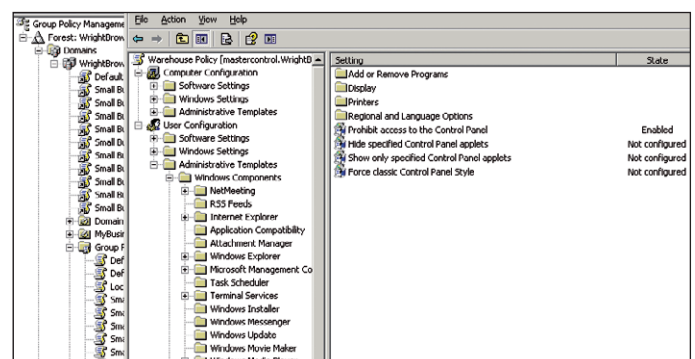
Once we've finished configuring the settings for our GPO, we simply close the Group Policy Object Editor and our changes will be saved automatically.

Next month

CONFIGURE MICROSOFT EXCHANGE
Get your email working smoothly with Microsoft's powerful email server



▲ You can't actually link a Group Policy Object directly to an Active Directory group, but using groups greatly simplifies the administration of Access Control Lists



▲ Using Group Policy you can specify precisely how a user interacts with their computer and with other objects on the network. You can even remotely install software using Group Policy